United States Department of the Interior

BUREAU OF LAND MANAGEMENT
Montana State Office
5001 Southgate Drive, P.O. Box 36800
Billings, Montana 59107-6800
http://www.mt.blm.gov/

In Reply To:

1278, 1400-735 (933.CS) P

March 23, 2005

EMAIL TRANSMISSION – 03/23/005
Instruction Memorandum No. 2005-027
Expires: 09/30/06

To: All Montana/Dakotas Employees

From: State Director

Subject: Internet Acceptable Use

The purpose of this memorandum is to remind employees that the Bureau has issued policy regarding acceptable Internet usage and to remind employees that access to the Internet belongs to the BLM. Washington Office Instruction Memorandum No. 2004-116, Internet Acceptable Use, dated March 1, 2004 (Attachment 1), provides employees with expected standards of behavior when using the Internet and informs employees that Internet use is being monitored through the use of a variety of tools and/or techniques such as intrusion prevention/detection, content filtering, and the monitoring of firewall logs and bandwidth utilization. Records generated on, received from, or stored on BLM's Information Systems are properties of BLM and are subject to Agency review.

Employees are prohibited from using the Internet, at any time, for activities that are illegal; e.g., gambling (5 CFR 735.201), or that are inappropriate or offensive to co-workers or the public, such as creating, viewing, storing, transmitting, sending, or intentionally receiving communications, files, or documents that are, or could be, interpreted as being intimidating, harassing, unlawful, or containing hostile, degrading, sexually explicit, pornographic, discriminatory, or otherwise offensive references or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation.

Each time you log onto a Montana/Dakotas (MT/DAKs) computer, you are required to acknowledge, by clicking on the pop-up box, that you understand your computer use is potentially being monitored and that you consent to such monitoring. Bureau of Land Management employees must understand that the Internet address of any site they visit, the length of time they view the site, and any images or documents that they view, print or download, will be recorded and potentially reviewed. Bureau of Land Management employees must also understand that the time they spend on the Internet is logged and subject to being monitored and reviewed.

The National IRM Center has dedicated a full time position to monitoring Internet activity of all employees using BLM equipment. Consequently, the number of reported cases of misuse has increased significantly. This information is being shared with the intent of preventing MT/DAKs employee's from being involved in an Internet abuse/misuse situation.

If you have any questions or concerns regarding BLM Internet policies, you may contact your supervisor or Chuck Sandau, Human Resources Specialist, at (406) 896-5264.

Signed by: Martin C. Ott

Authenticated by: Donna K. Zentz, MT-933

1 Attachment
1-WO IM No. 2004-116 (4 pp)

UNITED STATES DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT
WASHINGTON, D.C. 20240

March 1, 2004

In Reply Refer To:
1278, 1400-735 (550) P

EMS TRANSMISSION 03/01/2004
Instruction Memorandum No. 2004-116
Expires: 09/30/2005

To: AD's, SD's and CD's
Attn: All Bureau of Land Management (BLM) Employees

From: Assistant Director Information Resources Management

Subject: Internet Acceptable Use

Program Areas: All Program Areas

Purpose: This Instruction Memorandum (IM) transmits policy governing the acceptable use of the Internet by BLM employees. The purpose of this policy is to provide employees with standards of behavior when using the Internet. Each item in the policy is designed to strengthen the quality, and the integrity, and promote the efficiency of this resource while minimizing risks to BLM employees and the information systems.

This policy applies to all employees, contractors, volunteers, and other individuals (hereafter referred to as "employees") who are provided access to the Internet through the BLM's network. This policy incorporates the principles of the Department's existing Internet Acceptable Use policy which allows employees to use the Internet during non-duty time to develop or enhance search and retrieval skills if the use of the Internet will not cost the Government an additional fee, will not strain resources or reduce productivity, and will not bring discredit to the Department of the Interior (DOI) or the BLM. The DOI's policy is available on the DOI home page and it may be viewed through Internet Explorer at: http://www.doi.gov/footer/doi_aup.html%25. Any violations to this policy may subject the individual to disciplinary action, up to and including discharge from Federal service. Supervisors are encouraged to consult with their Human Resources office prior to taking any disciplinary action related to this policy.

Policy/Action: In order to ensure compliance with federal laws, earlier guidance, and to protect the BLM from being victimized by the threat of viruses or hacking into our systems, the following guidelines are hereby adopted:

- Employees are authorized to access the Internet for official business and for limited personal use during non-duty time in strict compliance with the other terms of this policy.

- Employees may not use the BLM's Internet for commercial gain or personal business.

- Employees are allowed to make some personal purchases through the Internet, but only during non-duty time. Employees are reminded that you may not use Government issued credit cards for personal purchases**.** Additionally, when making personal purchases, employees must have the purchases sent to a non-Government address.

- Employees are prohibited from using the Internet, at any time, for activities that are illegal; e.g., gambling (5 CFR 735.201), or that are inappropriate or offensive to co-workers or the public, such as or creating, viewing, storing, transmitting, sending, or intentionally receiving communications, files, or documents that are or could be interpreted as being intimidating, harassing, unlawful, or containing hostile, degrading, sexually explicit, pornographic, discriminatory, or otherwise offensive references or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin or sexual orientation.

- Employees are prohibited from using the Internet for any such activity that may damage the reputation of the BLM such as expressing personal views in a way that would lead the public to interpret it as an official government position. This includes posting opinions or statements to external news groups, bulletin boards, or other public forums represented as official government views unless these are a part of an employee's official job duties.

- Employees are prohibited at any time from using the Internet as a radio or music player. Such live stream use of the Internet could strain the BLM network and significantly slow communications, preventing BLM employees from conducting official business.

- Employees are prohibited at any time from participating in any unofficial chat rooms.

- Employees are prohibited from downloading "push" technology or continuous data streams from the Internet, unless they are directly associated with the employee's job. Push technology from the Internet includes any type of daily, hourly, streaming, or continuous updates from sources such as the news, stock quotes, weather, and similar information. BLM web pages will not contain presentations such as local weather, news broadcasts, or other features that requires video streaming technology. Continuous data streams adversely degrade network performance.

- Employees are prohibited from downloading unapproved software from the Internet. Prior to installing software on BLM systems, it must be approved by the local Chief Information Officer or their designated representative.
  All files that are installed upon BLM computer systems or are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to prevent the spread of viruses to BLM equipment and networks.

- Employees must exercise caution and care when utilizing the Internet. The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet is at risk of detection or interception by a third party.

- Employees may not intentionally intercept, eavesdrop, record, read, alter, or receive another person's Internet transmissions without proper authorization in accordance with this policy.

- Managers must remind employees that access to the Internet belongs to the BLM. By accessing the Internet through the BLM, employees are consenting to be monitored. BLM employees must understand that the Internet address of any site they visit, the length of time they view the site, and any images or documents that they view, print or download will be recorded and potentially reviewed. BLM employees must also understand that the time they spend on the Internet is logged and subject to being monitored and reviewed.

- Prior to adopting and/or implementing this policy, local management must fulfill its labor management obligations with their exclusive bargaining unit representative(s), as appropriate.

Time Frame: This policy is in effect immediately with the release of this IM.

Budget Impact: None**.**

Background: The BLM is committed to utilizing new technologies that enable BLM employees to achieve the Bureaus mission, objectives, and goals. This includes a cadre of communications tools such as telephones, (including cell phones and other wireless devices), voice mail, computers, facsimile machines, pagers, electronic mail (e-mail) systems, Internet access, and web browsers. These communications tools are BLM property and are primarily intended for business-related purposes. The BLM maintains the integrity of Internet use by using a variety of tools and/or techniques such as intrusion prevention/detection, content filtering, and monitoring of firewall logs and bandwidth utilization. Records generated on, received from, or stored on BLM's Information Systems are the property of BLM and are subject to be reviewed by the BLM. Some records may be considered private under the Privacy Act**.**

BLM published interim policy through Information Bulletins 99-190, 2001-132, and Instruction Memoranda 97-177, based on guidance issued in DOI IRM Bulletin 1997-01. This original policy was coordinated with employee bargaining units and was developed in consultation with the DOI's Office of the Solicitor. On June 14, 2000, the Office of Policy, Management and Budget issued Secretarial Memorandum "Policies on Limited Use of Government Equipment and Telephone Use" to clarify key terms and provide management with the mechanism to modify the policy as appropriate to their circumstances. BLM decided to adopt the policy as issued.

On August 9, 2002, BLM issued IM 2002-224 to enforce the existing Internet Acceptable Use Policy. Although this IM expired on September 30, 2003, the policy and methods put into effect remain in place. Human Resources Management and Information Resources Management Directorate's are encouraged to take the appropriate actions to update all affected Handbooks and Manuals based on the release of this policy. This initial guidance enabled employees to use the Internet to perform Bureau missions and to develop Internet skills to improve job related knowledge. This IM incorporates, and clarifies the initial policy. Several terms were defined in the initial guidance and still apply.

Terms:

- **Commercial gain activity** is defined as any activity involving or relating to buying, selling, advertising, leasing, or exchanging products or services for anyone's personal profit or gain. It includes day trading, selling items on auction sites such as eBay, and buying or selling real estate for commercial purposes.

- **Limited personal use** refers to any activity that is conducted for purposes other than accomplishing official or otherwise authorized duties which does not adversely affect the employee's job performance.

- **Non-duty time** is time when the employee is not expected to be performing official business. To the extent permitted by this policy, employees may, for example, use Government office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, weekends or holidays (if their duty station is normally available to them at such times).

Manual/Handbook Sections Affected: Human Resources Employee Orientation Guidance Chapter 3 Ethics and Personal Conduct, and Chapter 14 Information Technology (IT) Security at http://www.ntc.blm.gov/leadership/orientation.

Coordination: This IM was coordinated with Human Resources Management, BLM CIO Council, Information Technology Security, Investment Management Group, IRM Policy, DOI, Office of the CIO, State/National Center Configuration Managers, and the National Information Resources Management Center.

Contact: If you have any questions or concerns regarding this policy, you may contact your supervisor or Paulette Sanford at (202) 452-0309.

Signed by:
Michael J. Howell, Jr.
Acting Assistant Director
Information Resources Management

Authenticated by:
Barbara J. Brown
Policy & Records Group, WO-560